МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»

**Общий факультет (Фрязино)**

УТВЕРЖДАЮ

Директор филиала РТУ МИРЭА в г. Фрязино

_____ Макарова Л.А.

«___» _____ 2021 г.

# Рабочая программа дисциплины (модуля)
# Защита информации

| | |
|---|---|
| Читающее подразделение | **кафедра общенаучных дисциплин** |
| Направление | **09.03.01 Информатика и вычислительная техника** |
| Направленность | **Цифровизация предприятий в области радиоэлектроники** |
| Квалификация | **бакалавр** |
| Форма обучения | **очная** |
| Общая трудоемкость | **5 з.е.** |

**Распределение часов дисциплины и форм промежуточной аттестации по семестрам**

| Семестр | Зачётные единицы | Распределение часов | | | | | | | Формы промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|
| | | Всего | Лекции | Лабораторные | Практические | Самостоятельная работа | Контактная работа в период практики и (или) аттестации | Контроль | |
| 7 | 5 | 180 | 32 | 0 | 32 | 80 | 2,35 | 33,65 | Экзамен |

Москва 2021

Программу составил(и):

*старший преподаватель, Волков Владимир Николаевич* _____

Рабочая программа дисциплины
**Защита информации**

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 929)

составлена на основании учебного плана:
направление: 09.03.01 Информатика и вычислительная техника
направленность: «Цифровизация предприятий в области радиоэлектроники»

Рабочая программа одобрена на заседании кафедры
**кафедра общенаучных дисциплин**

Протокол от 30.08.2021 № 1

Зав. кафедрой Щучкин Григорий Григорьевич _____

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры
**кафедра общенаучных дисциплин**

Протокол от __ _____ 2022 г. № __

Зав. кафедрой _____ _____
Подпись Расшифровка подписи

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
**кафедра общенаучных дисциплин**

Протокол от __ _____ 2023 г. № __

Зав. кафедрой _____ _____
Подпись Расшифровка подписи

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
**кафедра общенаучных дисциплин**

Протокол от __ _____ 2024 г. № __

Зав. кафедрой _____ _____
Подпись Расшифровка подписи

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
**кафедра общенаучных дисциплин**

Протокол от __ _____ 2025 г. № __

Зав. кафедрой _____ _____
Подпись Расшифровка подписи

# 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Защита информации» имеет своей целью способствовать формированию у обучающихся компетенций. предусмотренных данной рабочей программой в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника с учетом специфики направленности подготовки – «Цифровизация предприятий в области радиоэлектроники».

# 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

| | |
|---|---|
| Направление: | 09.03.01 Информатика и вычислительная техника |
| Направленность: | Цифровизация предприятий в области радиоэлектроники |
| Блок: | Дисциплины (модули) |
| Часть: | Часть, формируемая участниками образовательных отношений |
| Общая трудоемкость: | 5 з.е. (180 акад. час.). |

# 3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

В результате освоения дисциплины обучающийся должен овладеть компетенциями:

**ПК-2** - Способен настраивать, тестировать, устранять неполадки и определять параметры безопасности и защиты программного обеспечения сетевых устройств и устройств информационных систем и информационно-коммуникационных систем

**ПК-4** - Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы

**ПК-1** - Способен проектировать, создавать и сопровождать информационные системы среднего и крупного масштаба и сложности

**ПК-3** - Способен управлять проектами в области информационных технологий

## ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), ХАРАКТЕРИЗУЮЩИЕ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

### ПК-1 : Способен проектировать, создавать и сопровождать информационные системы среднего и крупного масштаба и сложности

#### ПК-1.1 : Разрабатывает и создаёт информационные системы.

**Знать:**

- Языки программирования и работы с базами данных
- Современные структурные языки программирования
- Современные объектно-ориентированные языки программирования
- Сетевые протоколы
- Основы программирования
- Коммуникационное оборудование

**Уметь:**

- Кодировать на языках программирования

#### ПК-1.2 : Осуществляет модульное и интеграционное тестирование информационной системы(верификация). Оптимизирует работу и модифицирует информационные системы. Сопровождает приемо-сдаточные испытания и ввод в эксплуатацию системы.

**Знать:**

- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников

- Отраслевая нормативная техническая документация
- Основы современных операционных систем
- Основы информационной безопасности организации

**Владеть:**

- Изменение методов доступа к данным

**ПК-2 : Способен настраивать, тестировать, устранять неполадки и определять параметры безопасности и защиты программного обеспечения сетевых устройств и устройств информационных систем и информационно-коммуникационных систем**

**ПК-2.1 : Администрирует сети с целью управления доступом к данным, управления безопасностью сетевых устройств и программного обеспечения сетевых устройств**

**Знать:**

- Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных
- Сетевые протоколы
- Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
- Основы информационной безопасности организации
- Основные средства криптографии
- Защищенные протоколы управления

**Уметь:**

- Устанавливать права доступа к файлам и папкам
- Применять программные средства защиты сетевых устройств от несанкционированного доступа
- Применять программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа
- Применять аппаратные средства защиты сетевых устройств от несанкционированного доступа
- Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

**Владеть:**

- Документирование настроек средств обеспечения безопасности удаленного
- Оценка безопасности и защиты приложений от несанкционированного доступа
- Планирование защиты приложений от несанкционированного доступа
- Отмена прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС
- Назначение прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС
- Определение необходимого уровня прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС
- Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов)
- Установка дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация
- Параметризация операционных систем средств удаленного доступа
- Установка межсетевых экранов, гибких коммутаторов, средств предотвращения атак виртуальной частной сети
- Установка специализированных программных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа
- Параметризация операционных систем дополнительных средств защиты администрируемой сети от несанкционированного доступа
- Оценка защиты операционных систем от несанкционированного доступа

- Планирование защиты операционных систем от несанкционированного доступа

**ПК-2.2 : Развертывает информационные системы у заказчика и интегрирует информационные системы с существующими информационными системами заказчика : настраивает оборудования, устанавливает и настраивает системное и прикладное ПО, обучает пользователей. Оценивает производительность сетевых устройств и программного обеспечения информационных систем.**

**Знать:**

- Языки современных бизнес-приложений
- Основные принципы обучения
- Технологии подготовки и проведения презентаций
- Современный отечественный и зарубежный опыт в профессиональной деятельности
- Современные структурные языки программирования
- Современные объектно-ориентированные языки программирования
- Системы хранения и анализа баз данных
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Основы менеджмента, в том числе менеджмента качества
- Основы информационной безопасности организации

**Владеть:**

- Настройка ИС для оптимального решения задач заказчика
- Сбор замечаний и пожеланий пользователей для развития ИС
- Осуществление выходного тестирования пользователей ИС

**ПК-3 : Способен управлять проектами в области информационных технологий**

**ПК-3.1 : Организовывает заключения договоров в соответствии с полученным заданием, организовывает заключение дополнительных соглашений к договорам, организовывает мониторинг исполнения договоров и контроль поступления оплат по договорам, и закрытие договоров по факту выполнения работ. Осуществляет инженерно-техническую поддержку заключения договоров сопровождения инфомационной системы и дополнительных соглашений к договорам на выполняемые работы, связанные с инфомационной системой.**

**Знать:**

- Основы информационной безопасности организации
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников

**ПК-3.4 : Идентифицирует заинтересованные стороны проекта в области информационные технологии и анализирует риски в проектах в области информационных технологий в соответствии с полученным заданием. Планирует проект в соответствии с полученным заданием, организовывает исполнения работ проекта, собирает информацию для инициации проекта, управляет изменениями в проектах ,мониторит и управляет работами проекта, завершает проекты, организует приемо-сдаточных испытания (валидация) в проектах малого и среднего уровня сложности и обеспечивает качество в проектах в области информационных технологий в соответствии с установленными регламентами.**

**Знать:**

- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников

**Владеть:**

- Инициирование запросов на изменения (в том числе запросов на корректирующие действия, на предупреждающие действия, на исправление несоответствий)

**ПК-4 : Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы**

**ПК-4.1 : Осуществляет предконтрактную подготовку разработки информационной системы: определение первоначальных требований заказчика к информационной системе и возможности их реализации, адаптация бизнес-процессов заказчика к возможностям информационнй системы, инженерно-техническая подддержка подготовки коммерческого предложения заказчику на поставку, создание(модификацию) и ввод в эксплуатацию информационную систему.**

**Знать:**

- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников

**Владеть:**

- Информирование заказчика о возможностях типовой ИС и типовых технологиях ее создания (модификации) и ввода в эксплуатацию
- Информирование заказчика о возможностях типовой ИС
- Выявление первоначальных требований заказчика к типовой ИС

**ПК-4.2 : Идентифицурует конфигурации информационной системы, управляет сборкой базовых элементов выбранной конфигурации и ведёт отчетность по статусу конфигурации.**

**Знать:**

- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Основы конфигурационного управления
- Инструменты и методы выдачи и контроля поручений

**ПК-4.3 : Проводит аудит конфигурации информационной системы и реализует процесс контроля качества.**

**Знать:**

- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Основы конфигурационного управления

**ПК-4.4 : Организовывает репозиторий хранения данных о создании (модификации) и вводе информационнй системы в эксплуатацию и организовывает приемо-сдаточных испытания (валидация) информационной системы и проверяет реализацию запросов на изменения (верификацию) информационной системы.**

**Знать:**

- Основы информационной безопасности организации
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников

**Уметь:**

- Устанавливать права доступа на файлы и папки

**Владеть:**

- Определение прав доступа к репозиторию проекта
- Создание репозитория проекта для хранения базовых элементов конфигурации
- Определение прав доступа для репозитория хранения данных о создании (модификации) и вводе ИС в эксплуатацию

**В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) ОБУЧАЮЩИЙСЯ ДОЛЖЕН**

**Знать:**

- Основы конфигурационного управления
- Инструменты и методы выдачи и контроля поручений
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Языки современных бизнес-приложений
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Основы информационной безопасности организации
- Основы информационной безопасности организации
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Основы конфигурационного управления
- Технологии подготовки и проведения презентаций
- Основы информационной безопасности организации
- Основы менеджмента, в том числе менеджмента качества
- Основные принципы обучения
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Современные структурные языки программирования
- Современный отечественный и зарубежный опыт в профессиональной деятельности
- Современные объектно-ориентированные языки программирования
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Системы хранения и анализа баз данных
- Сетевые протоколы
- Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников
- Основы информационной безопасности организации
- Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
- Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных
- Основы информационной безопасности организации
- Отраслевая нормативная техническая документация
- Основы современных операционных систем
- Основные средства криптографии
- Современные объектно-ориентированные языки программирования
- Сетевые протоколы
- Языки программирования и работы с базами данных
- Современные структурные языки программирования
- Защищенные протоколы управления
- Коммуникационное оборудование
- Основы программирования

**Уметь:**

- Кодировать на языках программирования
- Устанавливать права доступа к файлам и папкам
- Применять программные средства защиты сетевых устройств от несанкционированного доступа

- Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
- Применять аппаратные средства защиты сетевых устройств от несанкционированного доступа
- Применять программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа
- Устанавливать права доступа на файлы и папки

**Владеть:**

- Инициирование запросов на изменения (в том числе запросов на корректирующие действия, на предупреждающие действия, на исправление несоответствий)
- Информирование заказчика о возможностях типовой ИС и типовых технологиях ее создания (модификации) и ввода в эксплуатацию
- Создание репозитория проекта для хранения базовых элементов конфигурации
- Выявление первоначальных требований заказчика к типовой ИС
- Информирование заказчика о возможностях типовой ИС
- Определение прав доступа к репозиторию проекта
- Определение прав доступа для репозитория хранения данных о создании (модификации) и вводе ИС в эксплуатацию
- Установка специализированных программных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа
- Установка межсетевых экранов, гибких коммутаторов, средств предотвращения атак виртуальной частной сети
- Оценка защиты операционных систем от несанкционированного доступа
- Параметризация операционных систем дополнительных средств защиты администрируемой сети от несанкционированного доступа
- Параметризация операционных систем средств удаленного доступа
- Документирование настроек средств обеспечения безопасности удаленного
- Изменение методов доступа к данным
- Установка дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация
- Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов)
- Настройка ИС для оптимального решения задач заказчика
- Определение необходимого уровня прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС
- Осуществление выходного тестирования пользователей ИС
- Сбор замечаний и пожеланий пользователей для развития ИС
- Назначение прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС
- Оценка безопасности и защиты приложений от несанкционированного доступа
- Планирование защиты операционных систем от несанкционированного доступа
- Отмена прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС
- Планирование защиты приложений от несанкционированного доступа

## 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

При проведении учебных занятий организация обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений и лидерских качеств.

| Код заняти | Наименование разделов и тем /вид занятия/ | Сем. | Часов | Компетенции |
|---|---|---|---|---|
| **1. Курс лекций** | | | | |

| | | | | |
|---|---|---|---|---|
| **1.1** | **Понятие Информационной безопасности (Лек).** Базовые понятия и определения, используемые в сфере информационной безопасности. Роль справочно аналитических материалов в принятии управленческих решений. Представление о моделях безопасности Языки программирования и работы с базами данных.Современные структурные языки программирования.Основы программирования.Основы современных операционных систем.Современные структурные языки программирования.Современные объектно-ориентированные языки программирования. Системы хранения и анализа баз данных. Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных. | 7 | 2 | ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2 |
| **1.2** | **Выполнение практических заданий (Пр).** Назначение и программирование серверов в Конфигурация МЭ | 7 | 2 | ПК-1.1 |
| **1.3** | **Выполнение домашнего задания (Ср).** Выполнение домашнего задания | 7 | 20 | ПК-1.1 |
| **1.4** | **Подготовка к аудиторным занятиям (Ср).** Повторение и изучение пройденного материала | 7 | 20 | ПК-1.1 |
| **1.5** | **Законодательный уровень информационной безопасности (Лек).** Методы и средства обеспечения информационной безопасности компьютерных систем. Разработка макетов справочно-аналитических материалов для принятия управленческих решений на основе законодательного уровня ИБ. Основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий. Изменение методов доступа к данным. Отраслевая нормативная техническая документация.Уметь пользоваться нормативно-технической документацией в области инфокоммуникационных технологий. Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников. Основы менеджмента, в том числе менеджмента качества. Основы информационной безопасности организации | 7 | 2 | ПК-2.2, ПК-3.1, ПК-3.4, ПК-4.1, ПК-4.3, ПК-4.4, ПК-4.2, ПК-2.1, ПК-1.2 |

| | | | | |
|---|---|---|---|---|
| **1.6** | **Наиболее распространенные угрозы информационной безопасности (Лек).** Основы безопасности жизнедеятельности в области профессиональной деятельности. Принципы проектирования, внедрения и эксплуатация в организации ИС и ИКТ. Методы проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятияю. Основы информационнойбезопасности организации. Языки современных бизнес-приложений.Технологии подготовки и проведения презентаций. | 7 | 2 | ПК-4.2, ПК-2.2, ПК-2.1, ПК-1.2 |
| **1.7** | **Распространение объектно-ориентированного подхода на ИБ (Лек).** Методы и средства обеспечения информационной безопасности компьютерных сетей и систем на административном уровне ИБ. Обзор справочноаналитических материалов для принятия управленческих решений на административном уровне. Основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий. Сетевые протоколы. Коммуникационное оборудование. Отраслевая нормативная документация.Основы информационнойбезопасности организации | 7 | 2 | ПК-4.2, ПК-4.3, ПК-4.4, ПК-3.4, ПК-3.1, ПК-2.2, ПК-1.1, ПК-1.2 |
| **1.8** | **Процедурный уровень информационной безопасности (Лек).** Методы и средства обеспечения информационной безопасности компьютерных систем на процедурном уровне. Проектирование, внедрение и эксплуатация в организации ИС и ИКТ на процедурном уровне | 7 | 2 | ПК-4.2, ПК-1.2 |
| **1.9** | **Основные программнотехнические меры безопасности информации (Лек).** Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам. Постановка и решение схемотехнических задач, связанных с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным. Знакомство с методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия | 7 | 2 | ПК-4.2, ПК-4.3, ПК-4.4, ПК-3.4, ПК-3.1 |

| | | | | |
|---|---|---|---|---|
| **1.10** | **Основные программнотехнические меры безопасности информации: идентификация и аутентификация; управление доступом" Анализ защищенности (Лек).** Основы безопасности жизнедеятельности в области профессиональной деятельности. Постановка и решениесхемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным. Принципы реализации и использования алгоритмов идентификации и аутентификации, управления доступом и процедур анализа защищенности. | 7 | 2 | ПК-4.2, ПК-1.1 |
| **1.11** | **Основные программнотехнические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись (Лек).** Основные понятия. Описывается протоколирование и аудит, а также криптографические методы защиты. Показывается их место в общей архитектуре безопасности. Методы шифрования. Криптографического контроля целостности. Цифровые сертификаты.Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников. Основные средства криптографии. | 7 | 2 | ПК-4.2, ПК-2.2, ПК-1.2, ПК-2.1 |
| **1.12** | **Основные программнотехнические меры безопасности информации: Экранирование, анализ защищенности (Лек).** Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность | 7 | 2 | ПК-4.2, ПК-2.1 |
| **1.13** | **Криптография: шифрование и обеспечение целостности (Лек).** Основные угрозы безопасности информации и возможные способы их реализации, методы и средства противодействия этим угрозам. Применять на практике собственные и классические алгоритмы криптографической защиты данных. Методы проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия с испльзованиемкриптографическихсистемзащиты. Современный отечественный и зарубежный опыт в профессиональной деятельности | 7 | 2 | ПК-4.2, ПК-2.2 |

| | | | | |
|---|---|---|---|---|
| **1.14** | **Протоколирование и аудит, шифрование, контроль целостности (Лек).** Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам в рамках реализации процедур протоколирования и аудита, контроля целостности (в т.ч. с использованием элементов шифрования). | 7 | 2 | ПК-4.2, ПК-2.2 |
| **1.15** | **Антивирусная защита компьютерных систем (Лек).** Принципы организации антивирусной защиты информационных систем. Типология вирусов. Достоинства и недостатки эвристических алгоритмов поиска вирусов. | 7 | 2 | ПК-4.2, ПК-3.1, ПК-3.4, ПК-4.3, ПК-4.4 |
| **1.16** | **Место информационной безопасности экономических систем в национальной безопасности страны (Лек).** Информационная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция информационной безопасности. Основные сведения и положения. | 7 | 2 | ПК-4.2, ПК-3.1, ПК-3.4 |
| **1.17** | **Анализ способов нарушений информационной безопасности (Лек).** Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем. | 7 | 2 | ПК-4.2, ПК-4.4, ПК-3.4 |
| **1.18** | **Виды противников или «нарушителей». Понятие о видах вирусов (Лек).** Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация. | 7 | 2 | ПК-4.2, ПК-2.2, ПК-2.1 |
| **1.19** | **Использование защищенных компьютерных систем. (Лек).** Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике. | 7 | 2 | ПК-4.2, ПК-1.1, ПК-1.2 |
| **2. Практические занятия** | | | | |
| **2.1** | **Выполнение практических заданий (Пр).** Назначение и программирование серверов в Конфигурация МЭ | 7 | 2 | ПК-4.4, ПК-1.1, ПК-2.1 |
| **2.2** | **Выполнение практических заданий (Пр).** Организация VPN | 7 | 2 | ПК-1.1, ПК-2.1, ПК-4.4 |
| **2.3** | **Выполнение практических заданий (Пр).** Удалённое управление. Получение ключей. | 7 | 2 | ПК-1.1, ПК-4.4, ПК-2.1 |
| **2.4** | **Выполнение практических заданий (Пр).** Построение крипто туннеля управления виртуальным стендом | 7 | 2 | ПК-1.1, ПК-2.1, ПК-4.4 |

| | | | | |
|---|---|---|---|---|
| **2.5** | **Выполнение практических заданий (Пр).** Разбор содержимого конфигурационного файла | 7 | 2 | ПК-4.4, ПК-2.1, ПК-1.1 |
| **2.6** | **Выполнение практических заданий (Пр).** Работа с командами в командной строке | 7 | 2 | ПК-1.1, ПК-2.1, ПК-4.4 |
| **2.7** | **Выполнение практических заданий (Пр).** Настройка Ethernet-Интерфейсов, маршрутизации | 7 | 2 | ПК-4.4, ПК-2.1 |
| **2.8** | **Выполнение практических заданий (Пр).** Настройка и использование NAT. Изменение методов доступа к данным | 7 | 2 | ПК-1.1, ПК-2.1, ПК-4.4, ПК-1.2 |
| **2.9** | **Выполнение практических заданий (Пр).** Настройка фильтров трафика списками доступа | 7 | 2 | ПК-4.4, ПК-2.1, ПК-1.1 |
| **2.10** | **Выполнение практических заданий (Пр).** Удаленное управление хостами Dionis по протоколу SSH и интерфейсу DiWeb | 7 | 2 | ПК-4.4, ПК-2.1, ПК-1.1 |
| **2.11** | **Выполнение практических заданий (Пр).** Создание VPN, построение туннелей между хостами Dionis | 7 | 2 | ПК-1.1, ПК-2.1, ПК-4.4 |
| **2.12** | **Выполнение практических заданий (Пр).** Установка и инициализация СКЗИ для шифрования трафика в туннелях | 7 | 2 | ПК-4.4, ПК-1.1, ПК-2.1 |
| **2.13** | **Выполнение практических заданий (Пр).** Установка и обновление версий ОС Dionis NX | 7 | 2 | ПК-1.1, ПК-2.1, ПК-4.4 |
| **2.14** | **Выполнение практических заданий (Пр).** Создание резервных копий конфигурационных файлов и данных | 7 | 2 | ПК-4.4, ПК-2.1, ПК-1.1 |
| **2.15** | **Выполнение практических заданий (Пр).** Отладка и контроль прохождения пакетов через хост Dionis | 7 | 1 | ПК-1.1, ПК-2.1, ПК-4.4 |
| **2.16** | **Выполнение практических заданий (Пр).** Управление конфигурацией через интерфейс DiWeb | 7 | 1 | ПК-4.4, ПК-2.1, ПК-1.1 |
| **3. Самостоятельная работа** | | | | |
| **3.1** | **Подготовка к аудиторным занятиям (Ср).** Повторение и изучение пройденного материала | 7 | 20 | ПК-4.4, ПК-4.1, ПК-2.2, ПК-2.1, ПК-1.2 |
| **3.2** | **Выполнение домашнего задания (Ср).** Выполнение домашней работы по выданным преподавателем вариантам | 7 | 20 | ПК-1.2, ПК-2.1, ПК-2.2, ПК-3.4, ПК-4.1, ПК-4.4 |
| **4. Промежуточная аттестация (экзамен)** | | | | |
| **4.1** | **Подготовка к сдаче промежуточной аттестации (Экзамен).** | 7 | 33,65 | ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2, ПК-3.1, ПК-3.4, ПК-4.1, ПК-4.3, ПК-4.4, ПК-4.2 |

| | | | | |
|---|---|---|---|---|
| **4.2** | **Контактная работа с преподавателем в период промежуточной аттестации (КрПА).** | 7 | 2,35 | ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2, ПК-3.1, ПК-4.1, ПК-3.4, ПК-4.3, ПК-4.4, ПК-4.2 |

# 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

## 5.1. Перечень компетенций

Перечень компетенций, на освоение которых направлено изучение дисциплины «Защита информации», с указанием результатов их формирования в процессе освоения образовательной программы, представлен в п.3 настоящей рабочей программы

## 5.2. Типовые контрольные вопросы и задания

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?
25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27. В чем заключается контроль участников взаимодействия?
28. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?
30. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
31. Какой процесс называется аутентификацией пользователя?
32. Какие схемы аутентификации вы знаете?
33. Что такое смарт-карты?

34.Какие требования предъявляются к современным криптографическим системам защиты информации?
35.Что такое симметричная криптосистема?
36.Какие виды симметричных криптосистем существуют?
37.Что такое асимметричная криптосистема?
38.Что понимается под односторонней функцией?
39.Как классифицируются криптографические алгоритмы по стойкости?
40.В чем заключается анализ надежности криптосистем?
41.Что такое дифференциальный криптоанализ?
42.В чем сущность криптоанализа со связанными ключами?
43.В чем сущность линейного криптоанализа?
44.Какие атаки изнутри вы знаете?
45.Какая программа называется логической бомбой?
46.Какими способами можно проверить систему безопасности?
47.Что является основными характеристиками технических средств защиты информации?
48.Какие требования предъявляются к автоматизированным системам защиты третьей группы?
49.Какие требования предъявляются к автоматизированным системам защиты второй группы?
50.Какие требования предъявляются к автоматизированным системам защиты первой группы?
51.Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52.Какие требования предъявляются к межсетевым экранам?
53.Какие имеются показатели защищенности межсетевых экранов?
54.Какие атаки системы снаружи вы знаете?
55.Какая программа называется вирусом?
56.Какая атака называется атакой отказа в обслуживании?
57.Какие виды вирусов вы знаете?
58.Какие вирусы называются паразитическими?
59.Как распространяются вирусы?
60.Какие методы обнаружения вирусов вы знаете?
61.Какая программа называется монитором обращения?
62.Что представляет собой домен?
63.Как осуществляется защита при помощи ACL -списков?
64.Какой список называется перечнем возможностей?
65.Какие способы защиты перечней возможностей вы знаете?
66.Из чего состоит высоконадежная вычислительная база (ТСВ)?
67.Какие модели многоуровневой защиты вы знаете?
68.В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
69.Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
70.Какие задачи решает система компьютерной безопасности?
71.Какие пути защиты информации в локальной сети существуют?
72.Какие задачи решают технические средства противодействия экономическому шпионажу?
73.Какой порядок организации системы видеонаблюдения?
74.Что включает в себя защита информационных систем с помощью планирования?
75.Какие условия работы оцениваются при планировании?
76.Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
77.Что такое мобильные программы?
78.Что такое концепция потоков?
79.Что представляет собой метод «песочниц»?
80.Что такое интерпретация?

81.Что такое программы с подписями?
82.Что представляет собой безопасность в системе Java ?
83.Назовите несколько примеров политик безопасности пакета JDK 1.2?
84.Какие международные документы регламентируют деятельность по обеспечению защиты информации?
85.Что понимают под политикой информационной безопасности?
86.Что включает в себя политика информационной безопасности РФ?
87.Какие нормативные документы РФ определяют концепцию защиты информации?

### 5.3. Фонд оценочных материалов

Полный перечень оценочных материалов представлен в приложении 1.

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 6.1. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

| Наименование помещений | Перечнь основного оборудования |
|---|---|
| Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | Мультимедийное оборудование, специализированная мебель, наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации. |
| Помещение для самостоятельной работы обучающихся | Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации. |

### 6.2. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Microsoft Windows. Договор №32009183466 от 02.07.2020 г.
2. Microsoft Office. Договор №32009183466 от 02.07.2020 г.
3. PuTTY. Свободное программное обеспечение (лицензия MIT)

### 6.3. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

#### 6.3.1. Основная литература

1. Щеглов А. Ю., Щеглов К. А. Защита информации: основы теории [Электронный ресурс]:Учебник для вузов. - Москва: Юрайт, 2021. - 309 с – Режим доступа: https://urait.ru/bcode/469866
2. Каширская Е. Н., Макаров М. А. Защита информации в информационно - управляющих системах [Электронный ресурс]:учебное пособие. - Москва: РТУ МИРЭА, 2020. - 67 с. – Режим доступа: https://e.lanbook.com/book/167621
3. Бабенко Л. К., Ищукова Е. А. Криптографическая защита информации: симметричное шифрование [Электронный ресурс]:Учебное пособие для вузов. - Москва: Юрайт, 2020. - 220 с – Режим доступа: https://urait.ru/bcode/452871
4. Внуков А. А. Основы информационной безопасности: защита информации [Электронный ресурс]:Учебное пособие Для СПО. - Москва: Юрайт, 2021. - 161 с – Режим доступа: https://urait.ru/bcode/475890
5. Внуков А. А. Защита информации [Электронный ресурс]:Учебное пособие для вузов. - Москва: Юрайт, 2021. - 161 с – Режим доступа: https://urait.ru/bcode/470131
6. Внуков А. А. Защита информации:учебное пособие для вузов. - М.: Юрайт, 2020. - 161 с.
7. Каширская Е. Н., Макаров М. А. Защита информации в информационно-управляющих системах [Электронный ресурс]:учебное пособие. - М.: РТУ МИРЭА, 2020. - – Режим доступа: https://library.mirea.ru/secret/26082020/2380.iso

8. Щеглов А. Ю., Щеглов К. А. Защита информации: основы теории:учебник для бакалавриата и магистратуры. - М.: Юрайт, 2020. - 309 с.
9. Тумбинская М. В., Петровский М. В. Защита информации на предприятии [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2020. - 184 с. – Режим доступа: https://e.lanbook.com/book/130184
10. Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:. - Санкт-Петербург: Лань, 2020. - 124 с. – Режим доступа: https://e.lanbook.com/book/133924

## 6.4. РЕКОМЕНДУЕМЫЙ ПЕРЕЧЕНЬ СОВРЕМЕННЫХ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. База данных Web of Science
   http://www.webofknowledge.com
2. Международный ресурс для поиска и обмена научными публикациями
   https://www.researchgate.net
3. Электроника НТБ - научно-технический журнал

   http://www.electronics.ru
4. Электронный фонд правовой и нормативно-технической документации Техноэксперт http://www.docs.cntd.ru
5. Информационно-справочный портал научных публикаций отечественных и зарубежных авторов «Google Академия»

   https://www.scholar.google.ru
6. Научная электронная библиотека http://www.elibrary.ru

## 6.5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Самостоятельная работа студента направлена на подготовку к учебным занятиям и на развитие знаний, умений и навыков, предусмотренных программой дисциплины.

В соответствии с учебным планом дисциплина может предусматривать лекции, практические занятия и лабораторные работы, а также выполнение и защиту курсового проекта (работы). Успешное изучение дисциплины требует посещения всех видов занятий, выполнение заданий преподавателя и ознакомления с основной и дополнительной литературой. В зависимости от мероприятий, предусмотреннх учебным планом и разделом 4, данной программы, студент выбирает методические указания для самостоятельной работы из приведённых ниже.

При подготовке к лекционным занятиям студентам необходимо:
перед очередной лекцией необходимо просмотреть конспект материала предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.
При подготовке к практическому занятию студенты имеют возможность воспользоваться консультациями преподавателя.

При подготовке к практическим занятиям студентам необходимо:
приносить с собой рекомендованную преподавателем литературу к конкретному занятию;
до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;
в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

в ходе семинара давать конкретные, четкие ответы по существу вопросов;
на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Студентам, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному практическому занятию, рекомендуется не позже чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изученную на занятии.

Методические указания необходимые для изучения и прохождения дисциплины приведены в составе образовательной программы.

## 6.6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБУЧЕНИЮ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Медиаматериалы также следует использовать и адаптировать с учетом индивидуальных особенностей обучения лиц с ОВЗ.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

**ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 3E71B80600020002CF46

Владелец: Макарова Людмила Александровна

Действителен с 21.09.2021 по 21.09.2022